



IAAS HANDLEIDING - SOPHOS FIREWALL



Cloud2 B.V.
Koelmalaan 350 - 5e verdieping
1812 PS Alkmaar

Contents

IAAS HANDLEIDING - SOPHOS FIREWALL	0
HANDLEIDING - SOPHOS FIREWALL	2
STANDAARD FUNCTIONALITEITEN	2
DNS	2
DHCP	2
BASIS INSTELLINGEN UITVOEREN	3
INTERNET BESCHIKBAAR MAKEN (MGMT MACHINE)	3
FIREWALL RULE TOEVOEGEN	3
INSTELLEN STANDAARD REGELS	5
REMOTE DESKTOP INSTELLEN (NAT RULE)	5
SSL VPN	6
L2TP IPSEC VPN	10
FIREWALL RULES	11
MASQUERADING RULE	11
WINDOWS VPN CLIENT	12
TOOLS	13
UPDATES	13
BACKUP CONFIGURATIE	13
CONNECTION TOOLS	14
LICENTIE	15
AANBEVELINGEN	15

HANDLEIDING - SOPHOS FIREWALL

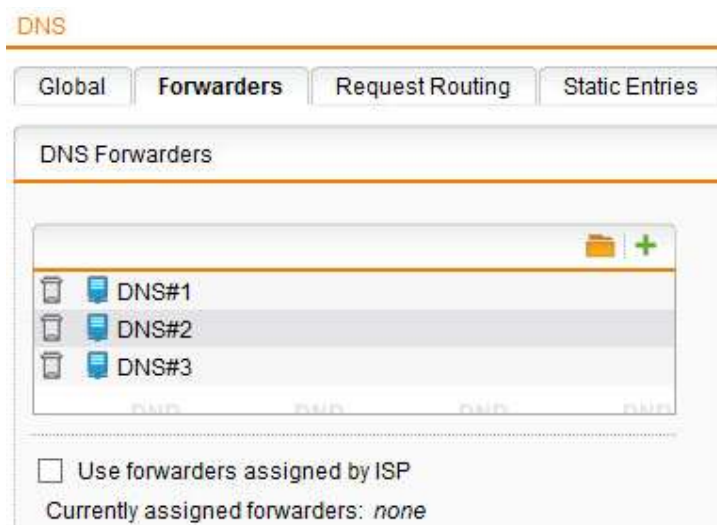
Wij raden voor onze klanten aan de Sophos UTM 9 firewall te gebruiken. Deze softwarematige firewall is voorzien van alle mainstream opties en mogelijkheden en zal voor het grootste deel van de klanten in ons systeem ruimte afdoende zijn om de wensen te vervullen.

In deze handleiding beschrijven we de standaard opties en firewall configuratie mogelijkheden.

STANDAARD FUNCTIONALITEITEN

DNS

Ga naar het menu 'Network Services > DNS > Forwarders' om de DNS settings van de firewall in te stellen. Schakel hier als eerste 'Use forwarders assigned by ISP' uit, we gaan de DNS Servers namelijk handmatig instellen.



Voeg de volgende drie DNS Servers van A2B Internet handmatig toe via het 'plus-icoon':

- 178.249.153.20
- 178.249.152.66
- 46.244.2.18

DHCP

DHCP is al via de Wizard bij het installeren van de machine in te stellen. De DHCP server is te vinden onder het menu 'Network Services > DHCP'.

Belangrijk voor de DHCP instellingen is dat de Gateway het ip-adres van de firewall is.

Via de tabbladen 'Lease Table' is in te zien welke adressen er uitgegeven zijn.

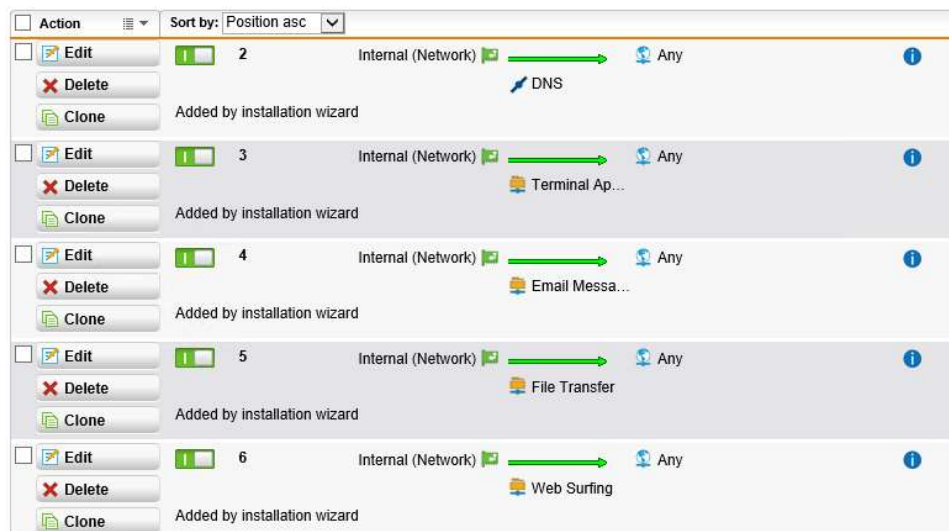
BASIS INSTELLINGEN UITVOEREN

INTERNET BESCHIKBAAR MAKEN (MGMT MACHINE)

Standaard worden de volgende protocollen vrijgegeven als de wizard wordt doorlopen:

- DNS;
- E-mail;
- FTP;
- HTTP / HTTPS.

De regels worden in het menu 'Network Protection > Firewall' als volgt weer te geven.



FIREWALL RULE TOEVOEGEN

In hetzelfde kan via 'New Rule' een nieuwe regel worden aangemaakt. Een nieuwe regel dient voorzien te worden van de volgende gegevens:

- Source: waar komt de traffic vandaan;
- Services: wat voor traffic is het;
- Destination: waar gaat de traffic naartoe.

Sources en Destinations: er zijn verschillende typen sources waar traffic vandaan gemanaged kan worden in de firewall:

- Host: een specifiek ip-adres;
- DNS Host / Group: een specifieke hostname;
- Network: een netwerk;
- Range: een selectie ip-adressen;

Services: er zijn verschillende typen services welke door de firewall gemanaged kunnen worden:

- TCP / UCP: standaard TCP en UDP services;
- ICMP / ICMPv6: monitoring software services;
- IP: zelf in te stellen services;
- Group: en selectie verschillende services.

Action: welke actie moet er gebeuren met de traffic die aan de gestelde eisen voldoet;

- Allow: laat het verkeer door;
- Drop: laat het verkeer vallen zonder terugkoppeling;
- Reject: blokkeer actief het verkeer

Advanced:

- Time period: wanneer is de regel actief?
- Log traffic: houd in een logfile bij welke traffic voldoet aan de eisen in de regel. Wij adviseren deze optie alleen aan te zetten wanneer er troubleshooting plaats vindt;
- Source MAC addresses: voeg MAC adressen toe van de devices die aan de regel moeten voldoen.



Group:

Position:

Sources:

DND	DND	DN
DND	DND	DN
DND	DND	DN
DND	DND	DN
DND	DND	DN
DND	DND	DN

Services:

DND	DND	DN
DND	DND	DN
DND	DND	DN
DND	DND	DN
DND	DND	DN
DND	DND	DN

Destinations:

DND	DND	DN
DND	DND	DN
DND	DND	DN
DND	DND	DN
DND	DND	DN
DND	DND	DN

Action:

Comment:

Advanced

Time Period:

Log traffic: ☐

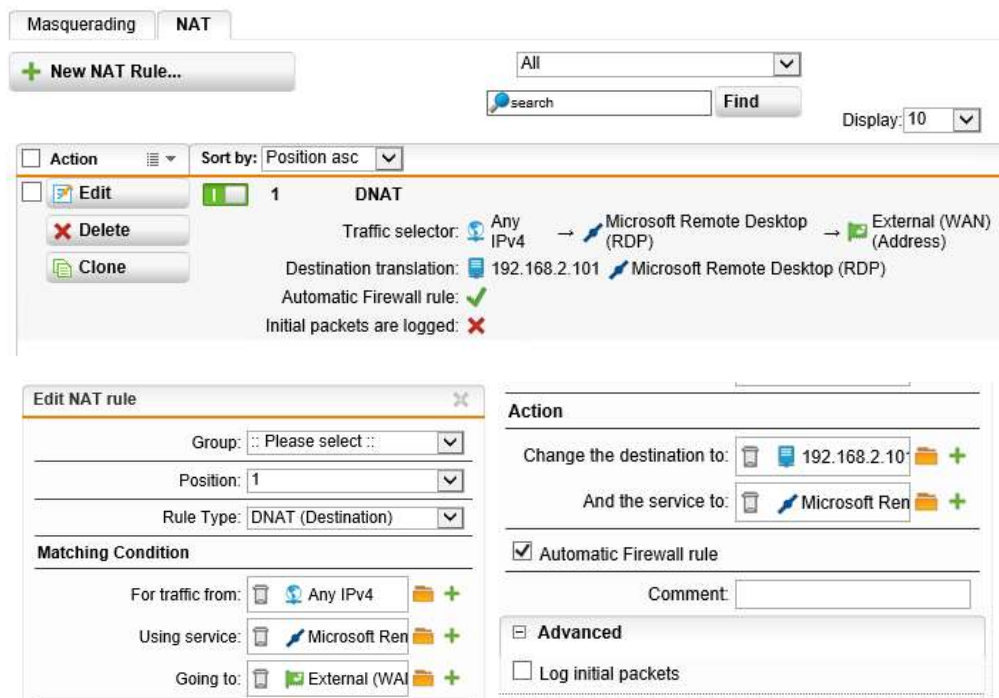
Source MAC Addresses:

INSTELLEN STANDAARD REGELS

REMOTE DESKTOP INSTELLEN (NAT RULE)

Het NAT menu is te bereiken onder 'Network Protection > NAT > Tabblad NAT'. Voeg daarna de volgende rule in om een RDP sessie naar een server toe te leiden.

Stel de regel als volgt in en zorg ervoor dat de optie 'Automatic Firewall Rule' is aangevinkt zodat de firewall automatisch wordt ingesteld om de traffic door te laten naar de juiste locatie.



The screenshot displays the NAT configuration interface. At the top, there are tabs for 'Masquerading' and 'NAT'. Below the tabs is a '+ New NAT Rule...' button. A search bar and a 'Find' button are also present. The main area shows a list of NAT rules, with one rule selected. The 'Edit NAT rule' dialog is open, showing the configuration for a DNAT rule. The 'Matching Condition' section shows 'For traffic from: Any IPv4', 'Using service: Microsoft Remote Desktop (RDP)', and 'Going to: External (WAN) (Address)'. The 'Action' section shows 'Change the destination to: 192.168.2.101' and 'And the service to: Microsoft Remote Desktop (RDP)'. The 'Automatic Firewall rule' checkbox is checked.

Wanneer deze regel voor meerdere servers aangemaakt moet worden, zorg er dan voor dat er per server een 'Service' voor de juiste poort wordt aangemaakt en dat de servers worden toegevoegd aan de 'Destinations'. Er kan dan per server een regel in de firewall gezet worden zodat alle servers van buitenaf via RDP te benaderen zijn.

SSL VPN

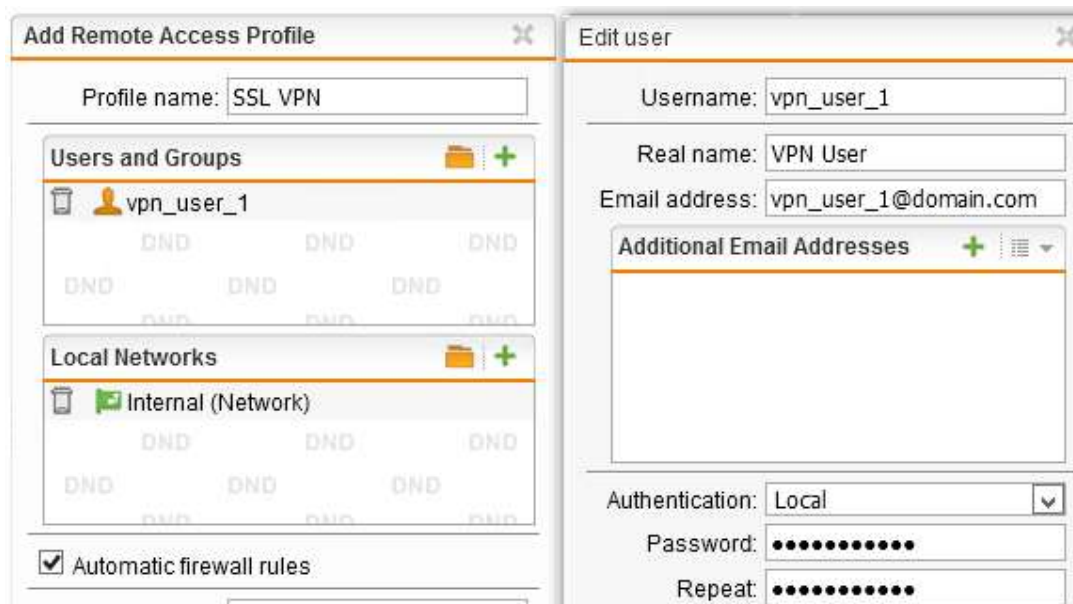
Sophos biedt de mogelijkheid om SSL VPN verbindingen op te zetten en clients op die manier makkelijk te laten verbinden met de omgeving.

Start door naar het menu 'Remote Access > SSL' te gaan en klik daar op 'New Remote Access Profile':



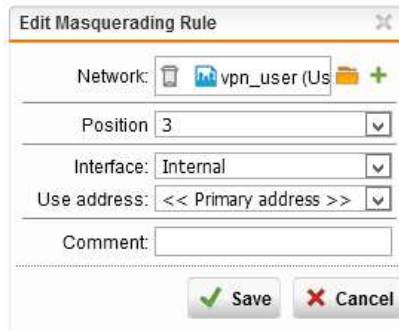
In het volgende menu moeten de volgende gegevens worden ingevoerd:

- Users en Groups: maak een nieuwe user aan;
- Local Networks: waar hebben de users toegang tot;
- Automatic firewall rules: laat deze aangevinkt.



Ga hierna naar het menu 'Network Protection > NAT > Masquerading' en stel daar in dat de VPN Users vanuit het interne netwerk moeten gaan communiceren.

Klik op 'New Masquerading Rule', geef de user of usergroup aan en selecteer bij interface de 'internal' interface:



Edit Masquerading Rule

Network: vpn_user (Us)

Position: 3

Interface: Internal

Use address: << Primary address >>

Comment:

Save Cancel

Controleer in het menu 'Network Protection > Firewall > Rules' of de firewall rule voor communicatie goed staat ingesteld:

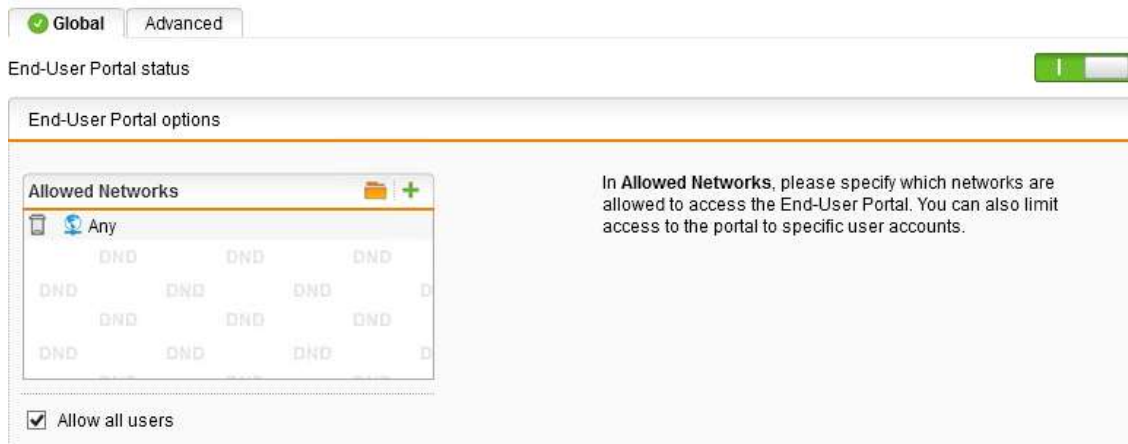


Edit 9 vpn_user (User Network) Internal (Network)

Delete Clone

Any

Ga nu naar het menu 'Management > User Portal' en geef aan dat de webportal gebruikt mag worden om op in te loggen en de SSL VPN software te downloaden:



Global Advanced

End-User Portal status

End-User Portal options

Allowed Networks

Any

DND DND DND

DND DND DND

DND DND DND

Allow all users

In **Allowed Networks**, please specify which networks are allowed to access the End-User Portal. You can also limit access to the portal to specific user accounts.

Ga hierna naar het externe ip-adres van de firewall en log daar in met de VPN gebruiker:



Login to UserPortal

Gebruikersnaam:

Wachtwoord:

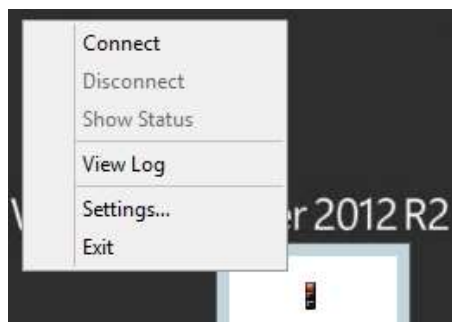
☐ Mijn login onthouden (in cookie)

Aanmelden

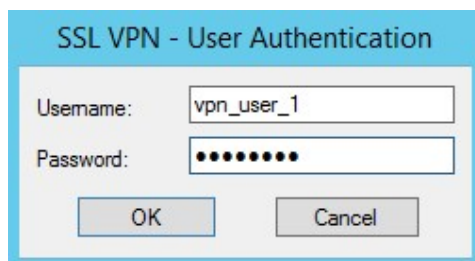
Onder het tabblad 'Externe toegang' kan de SSL VPN software gedownload worden:



Voer de .exe file uit en installeer de software. In de taakbalk verschijnt een icoon van een 'stoplicht', klik rechter muisknop > connect om verbinding te maken:



Vul in het volgende scherm de gebruikers gegevens van de vpn user in en klik op OK om verbinding te maken:



Als het icoon van de 'stoplicht' groen wordt is de verbinding in orde.

In het menu 'Remote Access > SSL > Settings > Virtual IP Pool' is de ip-adres pool aan te geven welke moet worden gegeven aan SSL VPN gebruikers:

Virtual IP Pool

Pool network:   VPN Pool (SSL) 

Duplicate CN

☒ Allow multiple concurrent connections per user

Edit network definition 

Name: VPN Pool (SSL)

Type: Network

IPv4 address: 10.242.2.0

Netmask: /24 (255.255.255.0)

Comment: Default SSL VPN IP Pool

Advanced

Interface: << Any >>

 Save  Cancel

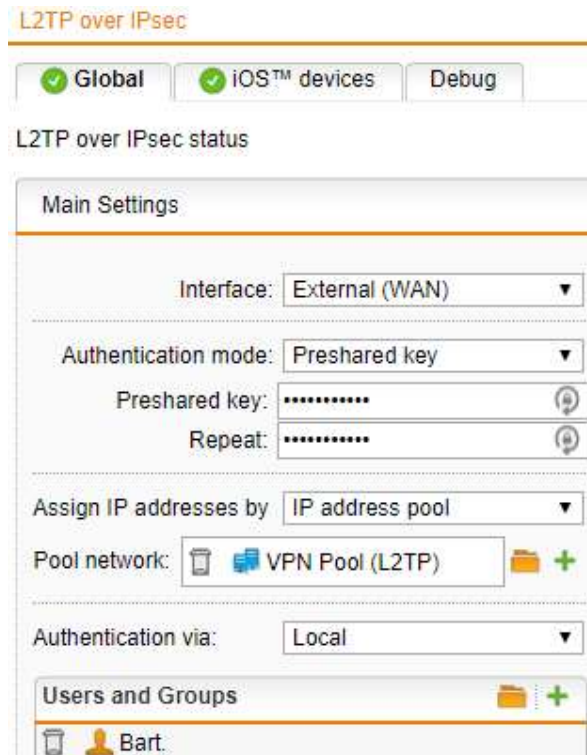
L2TP IPSEC VPN

Een L2TP over IPsec VPN verbinding is een perfecte manier om gebruikers direct vanaf hun client-device verbinding te laten maken met de omgeving.

In onderstaande screenshots laten we zien hoe deze in te stellen is.

Ga naar het menu 'Remote Access > L2TP over IPSEC' om de VPN verbinding te configureren.

Stel de configuratie als volgt in:



L2TP over IPsec

☒ Global ☒ iOS™ devices ☐ Debug

L2TP over IPsec status

Main Settings

Interface: External (WAN)

Authentication mode: Preshared key

Preshared key: [masked]

Repeat: [masked]

Assign IP addresses by: IP address pool

Pool network: [trash icon] VPN Pool (L2TP) [add icon]

Authentication via: Local

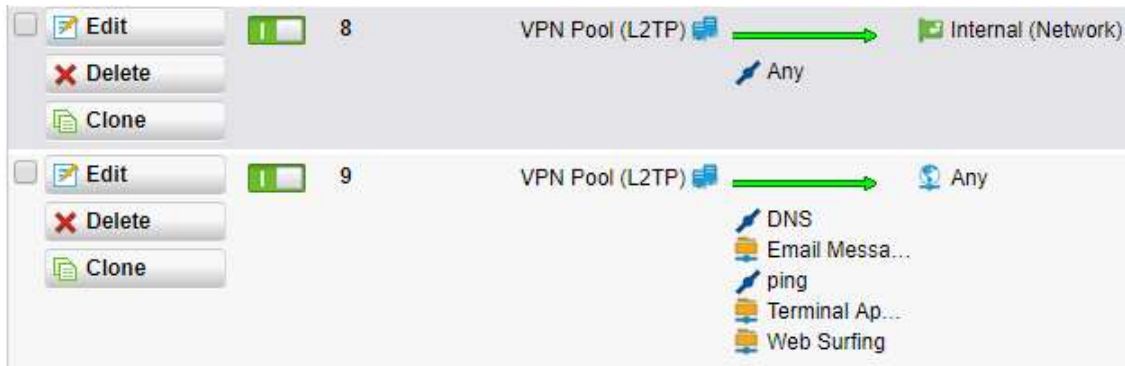
Users and Groups [add icon]

[trash icon] Bart

Voeg voor users die gebruik gaan maken van de VPN verbinding accounts toe.

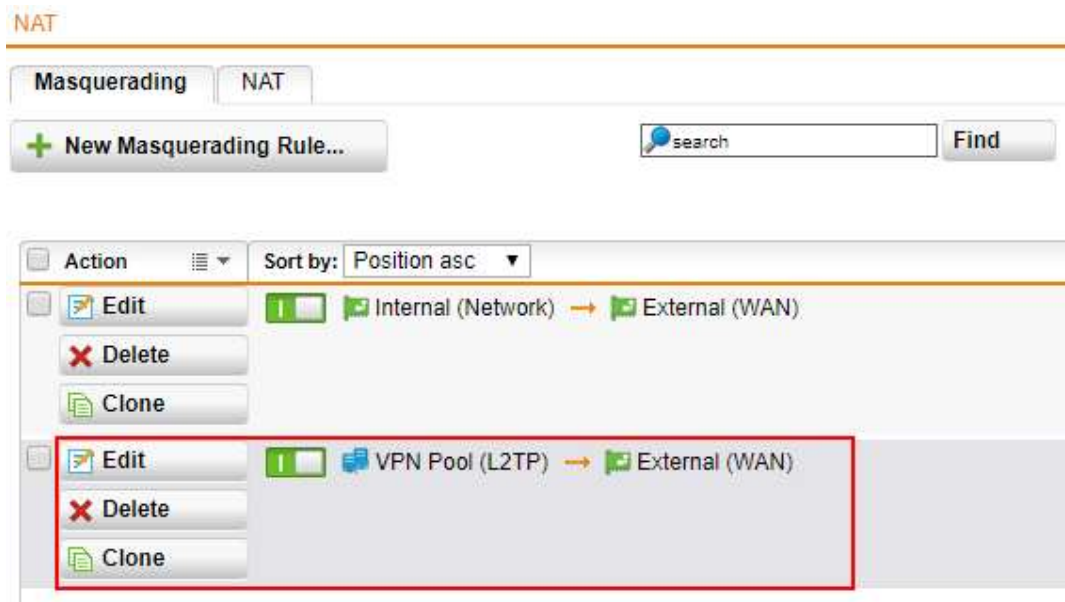
FIREWALL RULES

Stel de volgende firewall regels in om de gebruikers te kunnen laten internetten en standaard functionaliteiten te geven:



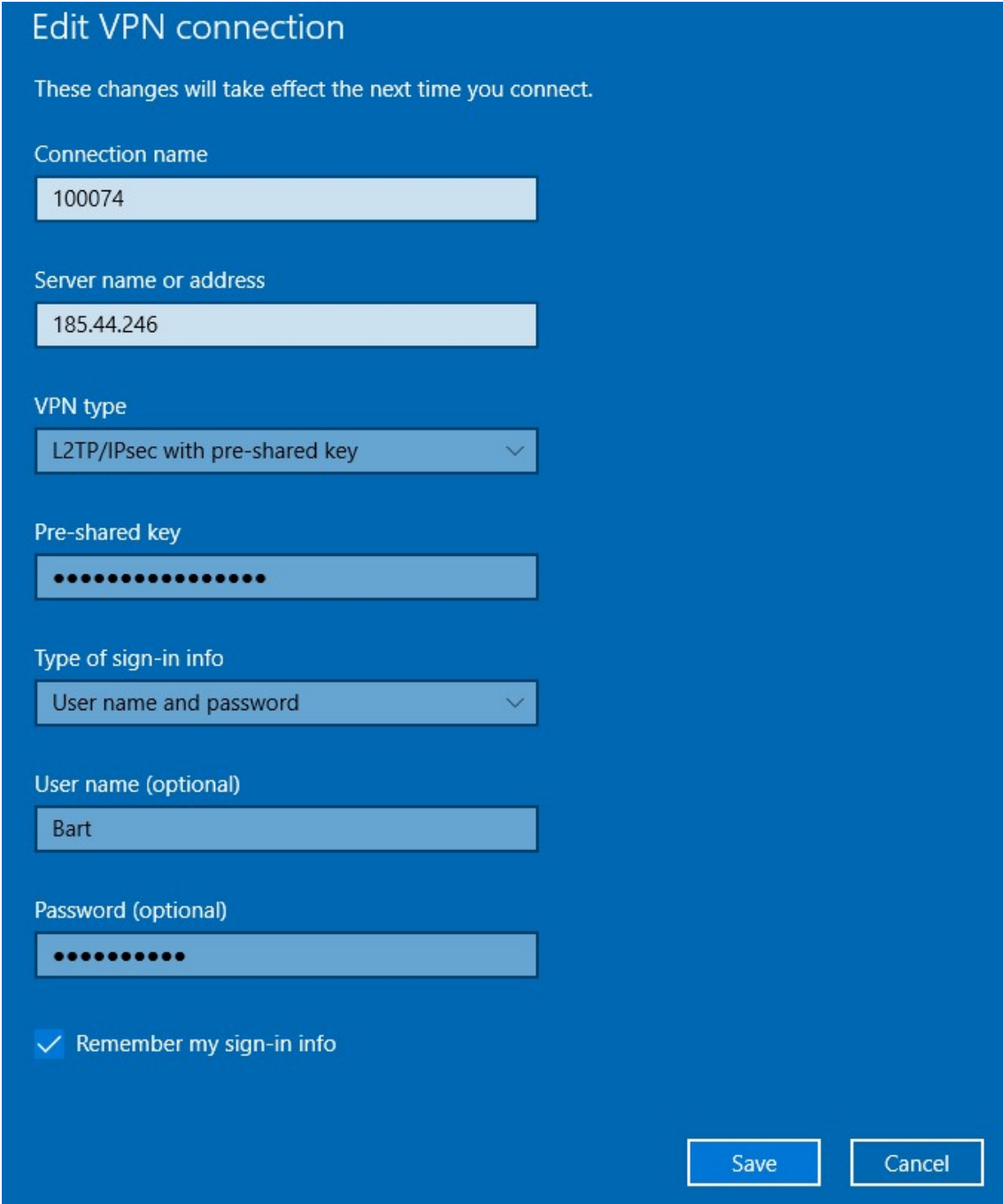
MASQUERADING RULE

Er dient een Masquerading rule aangemaakt te worden om de gebruikers te laten internetten vanuit VPN verbinding. Ga naar het menu 'Network Protecion > NAT > Masquerading' om deze aan te maken.



WINDOWS VPN CLIENT

In Windows kan de VPN verbinding nu worden ingesteld:



Edit VPN connection

These changes will take effect the next time you connect.

Connection name

100074

Server name or address

185.44.246

VPN type

L2TP/IPsec with pre-shared key

Pre-shared key

.....

Type of sign-in info

User name and password

User name (optional)

Bart

Password (optional)

.....

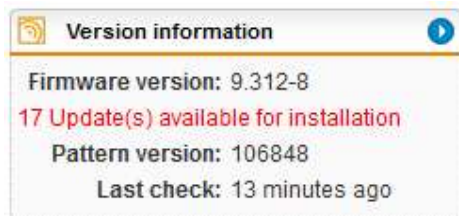
☒ Remember my sign-in info

Save Cancel

TOOLS

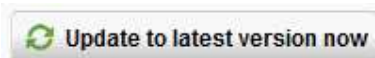
UPDATES

De Sophos firewall dient handmatig geupdate te worden. Of er een update beschikbaar is wordt weergegeven in de homescreen van de firewall onder 'Version information' of via het 'Management > Up2Date' menu:

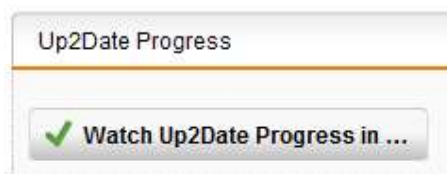


Klik op de rode regel waarin wordt aangegeven hoeveel updates er zijn om naar het totaaloverzicht te gaan.

Kies in het volgende scherm of alle updates in één keer moeten worden geïnstalleerd of dat ze per stuk geïnstalleerd moeten worden.



De voortgang kan worden bijgehouden via de optie 'Watch Up2Date Progress...'. Er zal een popup worden geopend waarin de installatie van de verschillende updates is bij te houden.



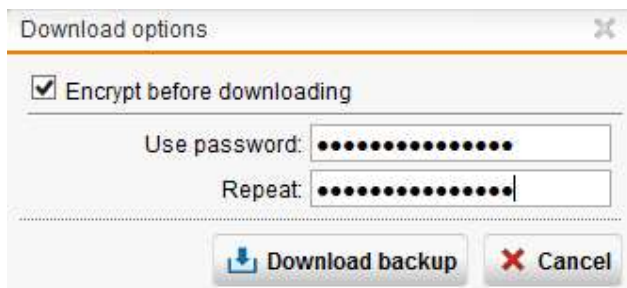
BACKUP CONFIGURATIE

Het is mogelijk om backups te maken van de configuratie van de firewall. Ga naar het menu 'Management > Backup/Restore'.

Er zijn drie opties onder dit menu:

- Available backups: geeft een overzicht van de beschikbare backups die hersteld kunnen worden;
- Create backup: geeft de mogelijkheid om handmatig een backup te maken;
- Import backup: geeft de mogelijkheid een backup van een configuratie terug te lezen.

Om een backup te maken, klik op het volgende icoon naast de juiste sessie: . Voer eventueel een encryptie wachtwoord in en klik op 'Download backup':



Download options

☒ Encrypt before downloading

Use password:

Repeat:

Download backup Cancel

Als u een backup wilt importeren dient u allereerst de backup-file te importeren naar de firewall. Klik op het 'folder-icoon' naast 'Backup File' en upload de juiste file. Voer eventueel het wachtwoord van de backup in en klik op 'Import Backup'.



Import Backup

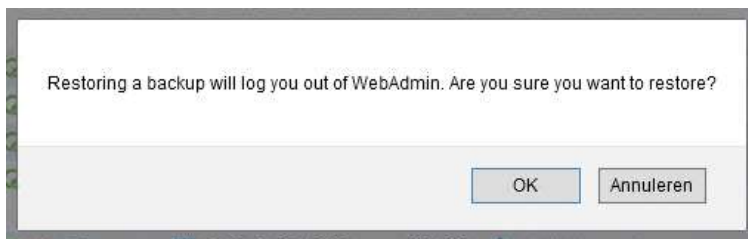
Backup file: fallback2.cloud2.nl_9.31:

Upload an existing **Backup file**. This will not instantly restore the backup, it will just be added to the list above.

Password:

Import Backup

De ingeladen backup komt nu in het overzicht van beschikbare backups te staan. Via het groene icoon  is de backup terug te zetten. De volgende melding komt naar voren:



Restoring a backup will log you out of WebAdmin. Are you sure you want to restore?

OK Annuleren

U zult uitgelogd worden en wanneer u daarna weer inlogt zult u de instellingen.

CONNECTION TOOLS

Tools om de verbinding te controleren zijn te vinden onder het menu 'Support > Tools'. Hier staan de volgende tools in:

- Ping Check: voert een ping naar een host of adres uit vanaf de externe interface van de firewall;
- Traceroute: voert een traceroute naar een host of adres uit vanaf de externe interface van de firewall;
- DNS Lookup: controleren ip-adres of hostname.

De meest gebruikte optie is de Ping Check, wanneer een server bijvoorbeeld geen internetverbinding lijkt te hebben is deze te gebruiken om te bepalen of de firewall zelf wel goed ingericht is en internet heeft.

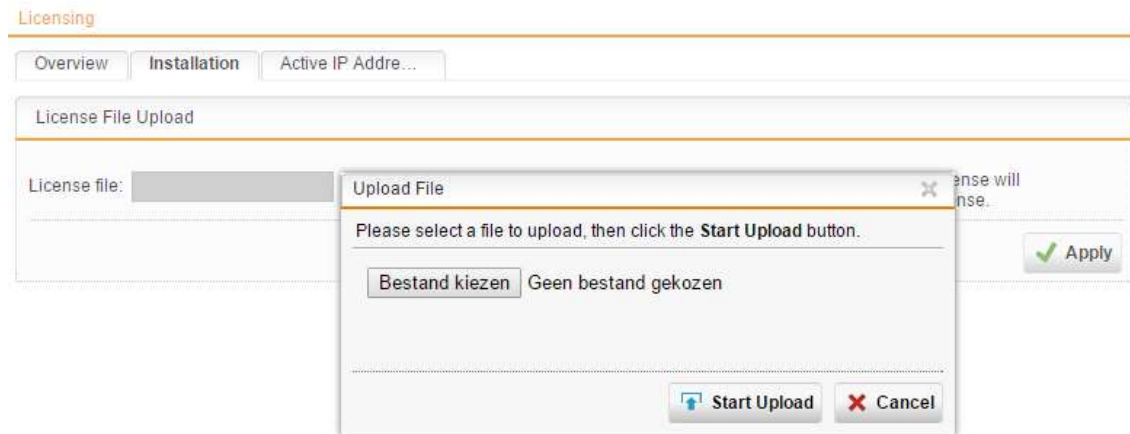
Voer een adres in en klik op 'Apply' om te controleren:



LICENTIE

Wanneer u een licentie wilt importeren gaat u naar het menu 'Management > Licensing > tabblad Installation'.

U kiest hier de licentie file (text bestand), upload de file en klikt op 'Apply' om hem in de server te importeren.



AANBEVELINGEN

De Sophos UTM firewall die geleverd wordt heeft een basic-configuratie, wij adviseren daarom een aantal wijzigingen door te voeren en in te regelen om het systeem veiliger te maken:

- Zorg dat servers niet via RDP op poort 3389 beschikbaar zijn;
- Stel Access Client Lists (ACL's) in voor personen die van buitenaf in mogen loggen;
- Wijzig de standaard wachtwoorden voor de webinterface en de root (SSH) login;
- Limiteer ook de toegang tot de web-interface met een ACL;
- Stel landenfilters in tegen hack pogingen uit andere delenv an de wereld;
- Zorg er altijd voor dat de firewall up-to-date is;
- Scherm NTP en DNS van buiten af.