KB 694838

Feste IP-Adressen auf Sophos UTM 9 einrichten (IKEIP)

Anleitung zur Einrichtung unseres Dienstes zur Bereitstellung von festen, öffentlichen IPv4-Adressen auf Sophos UTM 9 mit dem Einwahlserver IKEIP.

Code	694838
Stand	11.05.2018 20:39:50
Revision	5af5e376
Generiert	18.10.2018 13:21:52
ID	f608cfefd50ad744162594d678be2e5f
URL	http://www.feste-ip-adresse.net/kb/694838

Feste IP-Adressen auf Sophos UTM 9 einrichten (IKEIP)

Anleitung zur Einrichtung unseres Dienstes zur Bereitstellung von festen, öffentlichen IPv4-Adressen auf Sophos UTM 9 mit dem Einwahlserver IKEIP.

Vorwort

Alle Arbeiten geschehen auf eigene Gefahr. Diese Anleitung erhebt keinen Anspruch auf Richtigkeit oder Vollständigkeit. Für Schäden an Soft- und Hardware sowie für Ausfälle Ihrer Infrastruktur sind Sie selbst verantwortlich. Wir können keine Unterstützung für nicht von uns getestete Szenarien, Hardware, Software und Betriebssysteme anbieten. Alle Anleitungen setzen ein Blanko- bzw. minimal konfiguriertes System voraus. Bitte beachten Sie immer die Sicherheitshinweise in der Bedienungsanleitung des Herstellers. Führen Sie Tests nicht in Produktivumgebungen durch. Testen Sie die Lösung ausgiebig, bevor Sie sie produktiv einsetzen. Kritische IT-Systeme sollten nur von qualifiziertem Personal konfiguriert werden. Verwenden Sie stets sichere Passwörter, ändern Sie Standard-Passwörter umgehend ab.

Ziel dieser Anleitung ist es, unseren Dienst zum Erhalt von festen, öffentlichen IPv4-Adressen auf einer Sophos UTM 9 (ehemals Astaro) über eine IPsec Site-to-Site-Verbindung einzurichten.

Nach Abschluss der Anleitung liegen die Ihnen zugeteilten festen IP-Adressen auf der Sophos UTM 9 an. Außerdem wurde ein oder mehrere Server über NAT-Regeln mit jeweils einer festen IPv4-Adresse angebunden.

Bitte beachten Sie, dass diese Anleitung lediglich eine Empfehlung, ein getestetes und funktionierendes Referenz-Szenario, darstellt. Am Ende entscheiden natürlich Sie als Administrator welche Realisierungsform Sie verwenden möchten.

1. Policy definieren

Für die Verwendung unseres Dienstes wird eine eigene Policy benötigt, da Sophos UTM 9 keine passende Policy zur Verfügung stellt.

Menü: Site-to-site VPN > IPsec Reiter: Policies Aktion: New IPsec Policy…

Einstellungen:

1. Name: ikeip.internet-xs.de
2. IKE encryption algorithm: AES 256
3. IKE authentication algorithm: SHA256
4. IKE SA lifetime: 86400
5. IKE DH group: Group2: MODP 1024
6. IPsec encryption algorithm: No encryption (null)
7. IPsec authentication algorithm: MD5
8. IPsec SA lifetime: 86400
9. IPsec PFS group: None
10. Strict policy: Aktiviert
11. Compression: Deaktiviert

Klicken Sie auf “Save” um die Konfiguration zu speichern.

2. Remote Gateway definieren

Im nächsten Schritt wird das Remote Gateway – unser Einwahlserver – im System angelegt.

Menü: Site-to-site VPN > IPsec Reiter: Remote Gateways Aktion: New Remote Gateway…

Einstellungen:

1. Name: ikeip.internet-xs.de
2. Gateway type: Initiate connection
3. Gateway: Create New… (Plus-Zeichen). Ein überlagertes Fenster öffnet sich.

2.1 Host-Definition erstellen

Einstellungen:

1. Name: ikeip.internet-xs.de
2. Type: Host
3. IPv4 address: 212.58.69.60

Klicken Sie auf “Save” um die Konfiguration zu speichern, das überlagerte Fenster schließt sich wieder und das Host-Objekt wurde der Einstellung “Gateway” zugewiesen.

12. Authentication type: Preshared key
13. Key: PSK eingeben
14. Repeat: PSK nochmal eingeben
15. VPN ID type: Hostname
16. VPN ID: ikeip.internet-xs.de
17. Remote networks: Internet IPv4 (vorhandenes Objekt wählen)

Öffnen Sie den Abschnitt “Advanced”.

18. Support path MTU discovery: Aktiviert
19. Support congestion signaling (ECN): Deaktiviert
20. Enable XAUTH client mode: Aktiviert
21. Username: ixs060-nnnn-abcd0123
22. Password: YYYYYYYYYY
23. Repeat: YYYYYYYYYY

Klicken Sie auf “Save” um die Konfiguration zu speichern.

3. Connection definieren

Nachdem Policy und Remote Gateway definiert wurden, kann die Connection definiert werden.

Menü: Site-to-site VPN > IPsec Reiter: Connections Aktion: New IPsec Connection…

Einstellungen:

1. Name: ikeip.internet-xs.de
2. Remote gateway: ikeip.internet-xs.de
3. Local interface: WAN
4. Policy: ikeip.internet-xs.de
5. Local Networks: Create New… (Plus-Zeichen). Ein überlagertes Fenster öffnet sich.

3.1 Add network definition

1. Name: 212.58.80.XXX/YY (Netzadresse sowie Subnetzmaske in CIDR-Notation, die Sie von

uns erhalten haben)
2. Type: Network
3. IPv4 address: 212.58.80.XXX (Netzadresse, die Sie von uns erhalten haben)
4. Netmask: z.B. /29 (255.255.255.248) (Subnetzmaske, die Sie von uns erhalten haben)

Klicken Sie auf “Save” um die Konfiguration zu speichern, das überlagerte Fenster schließt sich wieder und das Host-Objekt wurde der Einstellung “Local Networks” zugewiesen.

6. Automatic firewall rules: Deaktiviert
7. Strict routing: Deaktiviert
8. Bind tunnel to local interface: Deaktiviert

Klicken Sie auf “Save” um die Konfiguration zu speichern.

4. Verbindung aktivieren

Die Konfiguration ist nun abgeschlossen. Aktivieren Sie die neue Verbindung in der Verbindungsübersicht durch klicken auf den Schalter. Der Schalter sollte anschließend grün werden.

5. Verbindung prüfen

Sie können nun prüfen, ob die Verbindung erfolgreich hergestellt wurde.

Menü: Site-to-site VPN

Es sollte ein neuer Abschnitt mit der Bezeichnung “ikeip.internet-xs.de” vorhanden sein. Dem Abschnitt sollte ein grüner Kreis mit einem Häkchen vorangestellt sein – außerdem sollte der Bezeichnung der Status “[1 of 1 IPsec SAs established]” angestellt sein. Ist dies der Fall wurde die Verbindung erfolgreich hergestellt.

6. Additional Addresses anlegen

Dieser Schritt ist über jede IPv4-Adresse aus dem Netz zu wiederholen, das Sie von uns erhalten haben. Bitte beachten Sie, dass Sie die Netzadresse sowie die Broadcast-Adresse nicht als Additional Address anlegen sollten.

Menü: Interfaces & Routing > Interfaces Reiter: Additional Addresses Aktion: New Additional

Address…

Einstellungen:

1. Name: 212.58.80.XXX+1
2. On interface: WAN
3. IPv4 address: 212.58.80.XXX+1
4. Netmask: /32 (255.255.255.255)

Klicken Sie auf “Save” um die Konfiguration zu speichern. Wiederholen Sie diese Schritte für alle weiteren festen IPs aus dem Ihnen zugeteilten Netz.

7. DNAT anlegen

Damit Traffic, der an 212.58.80.XXX geschickt und auf Ihrer Sophos UTM 9 landet auch zum richtigen Server geleitet wird, ist die Erstellung einer NAT-Regel erforderlich.

Menü: Network Protection > NAT Reiter: NAT Aktion: New NAT Rule…

Einstellungen:

1. Rule type: DNAT (destination)

8.1 Matching condition

2. For traffic from: Any IPv4 (vordefiniertes Objekt auswählen)
3. Using service: Der gewünschte Dienst, z.B. HTTPS (Port 443) (vordefniertes Objekt auswählen, alternativ neues Objekt anlegen)
4. Going to: 212.58.80.XXX (Netzobjekt einer Adresse, die als “Additional Address” erstellt wurde)

8.2 Action

5. Change the destination to: Host-Objekt / DMZ-LAN-IP-Adresse des anzubindenden Servers (ggf. erstellen)
6. And the service to: Leer
7. Automatic firewall rule: Aktiviert

Klicken Sie auf “Save” um die Konfiguration zu speichern. Wiederholen Sie diese Schritte für alle

Server und Dienste, die Sie mittels einer festen IP anbinden möchten.

8. SNAT anlegen

Damit Traffic, der an einen per DNAT angebundenen Server wieder mit der festen, öffentlichen IPv4-Adresse 212.58.80.XXX nach außen kommunizieren kann, ist die Verwendung von SNAT erforderlich.

Menü: Network Protection > NAT Reiter: NAT Aktion: New NAT Rule…

Einstellungen:

1. Rule type: SNAT (source)

8.1 Matching condition

2. For traffic from: Host-Objekt / DMZ-LAN-IP-Adresse des anzubindenden Servers
3. Using service: Der gewünschte Dienst, z.B. HTTPS (Port 443) oder Any (vordefniertes Objekt auswählen, alternativ neues Objekt anlegen)
4. Going to: Any IPv4

8.2 Action

5. Change the source to: 212.58.80.XXX (Netzobjekt einer Adresse, die als “Additional Address” erstellt wurde)
6. And the service to: Leer
7. Automatic firewall rule: Aktiviert

Klicken Sie auf “Save” um die Konfiguration zu speichern. Wiederholen Sie diese Schritte für alle Server und Dienste, die Sie mittels einer festen IP anbinden möchten.

A. Downloads

Diese Anleitung enthält keine Downloads.

B. Links

Diese Anleitung enthält keine Links.

Individuelle Beratung & Unterstützung

Zu unserem Service für Sie gehört eine individuelle Beratung und Unterstützung. Schildern Sie uns einfach kurz Ihr Anliegen und umschreiben Sie grob das Projekt, das Sie realisieren möchten. Gerne arbeiten wir mit Ihnen eine individuelle Lösung aus oder zeigen Lösungsmöglichkeiten auf.

Falls Sie sich bei der Kombination verschiedener Produkte nicht sicher sind, helfen wir Ihnen natürlich auch dabei gerne weiter.

Bei den meisten Tarifen bieten wir spezielle Konditionen für Reseller an. Bitte kontaktieren Sie uns für individuelle Angebote.

Im Falle von unerwarteten Problemen bei der Nutzung unserer Dienstleistungen stehen wir Ihnen selbstverständlich **auch nach der Bestellung** jederzeit gerne zur Verfügung.

Bei der Inbetriebnahme von bei uns bezogener und von uns konfigurierter Hardware oder bei der Inbetriebnahme reiner Software-Lösungen unterstützen wir Sie gerne, auch telefonisch.

Service für Geschäftskunden: Wir erstellen auch individuell Adressierte Komplettangebote in Textform, sofern dies für Ihren Einkauf benötigt wird.

Anfrage per E-Mail:
vertrieb@internet-xs.de

Telefonische Anfrage:

0711 / 78 19 41-0
zum Ortstarif, Geschäftszeiten: Werktags Mo. - Fr. 09:00 - 18:00 Uhr

Support per E-Mail:
support@internet-xs.de

Impressum

Internet XS Service GmbH

Heßbrühlstr. 15

70565 Stuttgart
Deutschland

Telefon: 0711 / 781941-0

Telefax: 0711 / 781941-79
E-Mail: vertrieb@internet-xs.de

Geschäftsführer: Helmut Drodofsky

Registergericht: Amtsgericht Stuttgart

Registernummer: HRB 21091
UST.IdNr.: DE 190582774

Alle Abbildungen ähnlich oder nur zu Illustrationszwecken.

Sofern nicht anders gekennzeichnet, **alle Preise inkl. 19% MwSt.**